

费者权利保护方面，民法调整的是平等主体的商家和消费者的关系，但是《民法通则》在制定时忽略了一点就是平等民事主体之间的关系可能有平等的关系和不平等的关系，很显然，商家在信息力等方面占有了绝对的优势，如果完全按照民法来调整的话显然不利于消费者利益的保护，这种情况下，就必须以国家或社会的力量涉入这一关系中，通过调整国家与商家的关系从而达到双方的平衡。随着生产社会化的发展，民法单纯的个人本位越来越表现出局限性，为适应不断发展的社会现实，民商法开始了现代化的进程，对个人本位做出了一定的修正，通过公序良俗等原则的确立，体现了对社会利益的一定关注。但是民商法的基础仍然是私权神圣、意思自治、契约自由，因而民商法不可能给与社会利益以充分的保护。经济法从产生起就以社会整体利益的实现为其使命，它要求个体和局部利益服从社会整体利益，短期利益服从长远利益。

经济法是由于近代生产社会化的大发展，国家为避免市场机制的缺陷给经济造成的失调而产生的，因此传统的经济法学者对经济法的研究不可避免地集中于如何进行市场规制和宏观调整方面上。当代社会，随着市场经济全球化和高新技术的突破性发展，经济的飞速发展使经济活动由个体经济发展为整体经济。经济活动以家庭、企业、个体利益为重心让位与整体利益为中心并要求从法律上加以确认；经济发展的目标是社会再生产的良性循环。相应地，经济法也空前繁荣，并凸显出自己不可替代的特点，是国家经济发展战略的保障。相应地经济法的基本特征更加明显，即综合调整，公法与私法互相渗透和社会责任本位。与其他部门法相比，经济法对弱势群体保护的视角具有经济性、宏观性，充分体现了经济法的社会本位性，进一步说明经济法的调整对象是特定的经济关系，而不是所有的经济关系；经济法的本质是国家从社会整体利益出发调控社会经济，使之良性运行、协调发展之法。目前在中国的经济转型时期社会性弱势群体的出现与经济体制、经济结构的不完善是分不开的，因此经济法必须尊重各经济主体的经济自由，维护其经济权利，要控制国家调节管理主体的权力，防止滥用。效益与公平是经济法基本价值。经济法要协调个体与社会总体的经济效益和利益，不能偏废；要维护社会各主体间的实质公平。相应地，对弱势群体的保护成为经济法研究中的新亮点。通过以上分析可以看出，经济法的研究范围是非常广泛的，并且随着经济生活的发展，其内容也不断丰富和扩冲，但并不意味着经济法无所不包。我们必须采取谨慎的态度去对待，不能想当然地为其研究领域于其他部门法去争执，以免使经济法处于包罗万象的尴尬境地。

参考文献：

1. 《经济法通论》 中南政法学院经济法系编 经济科学出版社 1986 年
2. 《经济法学评论》 史际春主编 中国法制出版社 2000 年
3. 《社会保障制度改革》 张琪，刘雄主编 经济管理出版社 1996 年
4. 《社会保障学：理念、制度、实践与思辨》 郑功成著 商务印书馆 2000 年
5. 《社会保障法》 覃有土，樊启荣编著 法律出版社 1997 年
6. 《经济法的理论问题》 梁慧星，王利明著 中国政法大学出版社 1986 年

Spam Solutions: A Law and Economics View

Li Xingan*

LI, Xingan (2005), Spam Solutions: A Law and Economics View, Asian and Comparative Law, Vol. III, No. 1, 2005.

Abstract: The paper begins with a precise description of the phenomenon, and continues in section II to classify the Spam. In Section III, the paper lists the problems brought about by Spam, such as fraud and deception, pornography, security implications and identity theft. Section IV gives a sketch of the scale of Spam. Section V is an analysis of the costs and benefits of sender and recipient of Spam. The paper examines

* Researcher, Faculty of Social Sciences, University of Joensuu, Finland.

effect of the four primary solutions, including technological, market, educational and regulatory in Section VI and VII. Special reference is placed on the economics analysis of different regulatory modes. At last, the paper ends with conclusions that Spam must be eliminated by comprehensive mechanisms.

Key words: direct marketing, Spam, law and economics

JEL Codes: D18, K14, K42, M31

I Introduction

As the increase of capability of computers and the networks to generate, store, and transmit information, "a wealth of information" can lead to a "poverty of attention" (Simon 1982). Pool et al. (1984) demonstrated that the supply of information has been growing faster than people's ability to consume it.

There are about 683 million E-mail users worldwide with nearly 1.2 billion active E-mail accounts in April 2005. These users send and receive 130 billion E-mail messages per day, although two thirds of that is Spam (Radical Group 2005). Forrester (Niall 2000) describes E-mail marketing as one of the most effective online marketing tools, and expects E-mail marketing to be worth \$5 billion by 2004. Peppers and Rodgers (2000, p 4) claim that "clear benefits, including high response rates and low costs are rapidly turning E-mail marketing into an invaluable tool".

However, Spam sent out to multiple recipients, stains the name of E-mail marketing; to avoid being perceived as Spam, authors suggest firms should restrict the messages they send (Wreden 1999; Wright and Bolfing 2001). Research (IMT Strategies 2001) found a growth in unopened E-mails, and increased action on the part of consumers to limit or remove most commercial online relationships.

Once considered minor nuisance, Spam has proven to be an increasingly large problem. In an Infoworld article (2003), over 40% of respondents listed Spam as the worst IT problem of the previous year. The scale and effect of the Spam prevalence implies that Spam has become "significant and growing problem for users, networks and the Internet as a whole" (WSIS Declaration, paragraph 37)

Most people have some unclear awareness that it came from at first from the "Spam skit by Monty Python's Flying Circus" (Templeton 2003). However, the history of Spam can be traced back to the late 1970's with BBSs, MUDs and MUSHes and USENET groups that were sent multiple mailings by the likes of Canter and Siegel, Rob Noha, and Dave Rhodes. These early mass mailings were not considered Spam at first but subsequently spread wide on the Internet (Templeton 2003). Templeton (2003) cites an example of E-mail Spam sent by DEC in 1978. Kelly (2002) explored the history of Spam and believes that it was born on 12 April, 1994. Spam came to prominence after the Canter and Siegel incident (Kelly 2002).

MAPS (2004) defines Spam as:

"An electronic message is "Spam" if: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; and (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender."

During the Geneva phase of the World Summit on the Information Society (WSIS), Spam was identified as a potential threat to the full utilization of the Internet and e-mail (ITU 2004a).

After giving a precise description of the phenomenon, the paper continues in section II to classify the Spam. In Section III, the paper lists the problems brought about by Spam, such as fraud and deception, pornography, security implications and identity theft. Section IV gives a sketch of the scale of Spam. Section V is an analysis of the costs and benefits of sender and recipient of Spam. The paper examines effect of the four primary solutions, including technological, market, educational and regulatory in Section VI and VII. Special reference is placed on the economics analysis of different regulatory modes. At last, the paper ends with conclusions that Spam must be eliminated by comprehensive mechanisms.

II Classification

Due to the complexity of the phenomenon, Spam can be classified in different ways. The delivery mode of Spam includes through E-mails, newsgroups, mobile phones Short Message Service (SMS) and instant messenger services (Batista 2000). The sender of Spam can be classified as strangers, acquaintances, and subscription services (Hise 1999). The content of Spam can be classified as commercial, political, industrial, chain mails, and others such as self-spreading virus E-mails (Foster 2000).

The US Federal Trade Commission identified twelve most likely Spam scams: business opportunity scams, making money by sending bulk E-mailing, chain letters, work-at-home schemes, health and diet scams, easy money, get something for free, investment opportunities, cable descrambler kits, guaranteed loans or credits on easy terms, credit repair scams, and vacation prize promotions (FTC 1998).

The sender's motive can be classified as informational, disrupting the working of a recipient or E-mail service provider's (ESP) network, and confusing or misinforming the recipients.

Classification of Spam is vital from a legal standpoint, because most Spam legislation targets a particular type, such as business E-mails, or deceptive Spam.

III Problems related to spam

1 Fraud and deception

66% of Spam messages are fraudulent in their "from" or "subject" lines, or in the message itself (FTC 2003b). Spammers disguise the origin of their messages because Spammers know their messages are being blocked or filtered; and aim to entice individuals to open their messages. These kinds of problems include false "from" and "reply-to" addresses, false routing information, deceptive subject lines, and fraudulent removal representations (FTC 2003a). It is also commonplace for Spam to include deceptive or misleading representations in the body of the message, such as the Nigerian scam, those promoting pyramid and bogus no-risk investment schemes, advertising "miracle" diets and health products, credit card or credit improvement offers, attractive travel packages or business opportunities, and messages promoting prostitution, illegal online gambling services, drugs or weapons sales, etc.

2 Pornography

Spam messages containing pornographic photographs, and promoting adult entertainment products and services are not appropriate for children. Since many Spammers do not target specific recipients, young children are likely to be inadvertently exposed to pornographic or offensive messages.

3 Security implications

Spam can clog up computer networks and temporarily paralyzes or even permanently damage personal computers when used to spread computer viruses or worms. Large volumes of Spam can interfere with critical computer infrastructures and endanger public safety.

Some Spam contains destructive viruses and worms. Brightmail (2003) estimated that 90% of viruses are passed through E-mail. 51% of corporations have had a virus disaster, and computer worms have become prevalent and problematic as well. Files such as spyware can be downloaded with the content of E-mail messages. Spammers also exploit security weaknesses inherent in E-mail transfer technology such as open relays and open proxies. According to MessageLabs, more than 60% of the Spam it traps each month is sent via open proxies (PC World 2003). The linkages between Spammers and writers of malicious code seem to be increasing. Other security issues are raised by the use of Spam to attract unsuspecting users to Web pages where spying software is secretly downloaded.

4 Identity theft

Identity theft is threatening e-commerce by corroding consumer trust. Spammers usually use some other business's IP address or conceal their own identity by using stolen or falsely labelled company identities. Individuals and organizations can be victims of identity theft. Many Spammers send their messages by using someone else's account without permission (OECD 2004).

Spyware can gather and transmit information about a user's activity on the Internet and information about E-mail addresses, passwords, and credit-card numbers (Boldt, Carlsson & Jacobsson 2004, p.8).

IV Scale of Spam

The ease of using Spam to offer goods and services increases the volume of Spam. Jupiter Communications foresees a forty-fold increase in Spam between 1999 and 2005, from 40 pieces to 1,600 pieces received per person annually (Marlin 2000).

According to IDC, a typical organization of 1000 people will receive and circulate 2.1 million Spam messages every year (Equip Technology & CipherTrust 2004). According to MessageLabs, the average global ratio of Spam to desired e-mails was 94.5% in July 2004 (compared to 52.8% in March 2004) (Equip Technology & CipherTrust 2004). Sophos statistics show that global Spam at the end of 2004 has reached 3 trillion messages, with an estimated cost of USD 131 billion and that volumes have doubled compared to the end of 2003 (Equip Technology & CipherTrust, 2004).

V Spam -Externalities in cyberspace

Externalities are defined by economists as the situation in which benefits and profits come by imposing cost on others. Externalities arise when two or more parties want to use the same scarce resource for conflicting purposes. Externalities are an inevitable result of common access to the Internet, a system comprised of scarce resources. Indeed, as more and more uses of this resources are discovered, and more and more people enter the commons, it is not at all surprising to find increasingly costly externality problems arising. People want to use this resource to lower their costs of buying or selling goods and services, to transmit and store data, to communicate with friends and colleagues, and for entertainment, but some people also get pleasure from causing harm to others. The net is sufficiently large to support tremendous numbers of activities, but crowding is becoming an increasingly significant problem (Wikipedia 2005).

In the case of spammers the costs to the recipients are much greater than the costs of the sender. Spamming shifts advertising costs from advertisers to both Internet users and ISPs. This cost-shifting may occur through higher subscription fees, or increased costs to ISPs for disk storage space, anti-spam enforcement, consumer complaints, and system delays (Amaditz 1999).

1 The costs and benefits of the sender

Khong (2004) claims that Spammer will undertake a Spamming activity if the expected benefit outweighs the cost. A Spammer only realizes his benefits when there is a successful commercial transaction following the Spam. However, it is difficult to measure the costs and benefits of the Spammer. A few empirical studies reported the average cost and benefit of a single message.

First, the Detroit Free Press reports (Wendland 2002) that Alan Ralsky, a notorious Spammer, charges \$22,000 to send to his entire database of 250 million addresses, or just about .01 cents per message. The New Zealand Herald (Griffin 2003) reports that one Spammer is paid US\$300 per million messages (.03 cents). In a New York Times interview, Spammer Richard Colbert says that he used to charge \$900 for one million Spams: about .1 cents per message. However, Colbert reports that prices have dropped precipitously recently, as low as \$25 per million: .0025 cents per message (Hansell 2003b).

Second, an article in the Hartford Courant (Moran 2002) says that Ronnie Scelson has revenue of \$30,000 to \$40,000 per 80 million messages, for revenue of as much as .05 cents per message, but is willing to Spam for products that bring as little as \$1000 per mailing (presumably also to 80 million people, or as little as .00125 cents). A Wall Street Journal Article says that Howard Carmack earned \$360 for sending 10 million messages, or .0036 cents per message (Grimes 2003).

Computer technology has cut the cost of delivering messages. Relative to the fixed cost of hardware and software, the marginal cost of delivering an electronic mail message is negligible. Hansell finds that the marginal cost of sending a marketing message to 1 million recipients by electronic mail is less than \$2,000, while the same solicitation sent by conventional, bulk-rate postal mail would cost over \$190,000 in postage, not counting paper and printing costs (Hansell 2003b). In the face of these low costs, it is economically rational for individual commercial E-mailers to distribute their messages as widely as possible. Experts estimate that commercial E-mail is profitable if even one recipient in 100,000 makes a purchase (Hansell 2003b).

In sum, the fact that the spam can be sent at very low cost and in a great quantity has attracted direct marketing companies to use Spam e-mails for advertisement.

2 The costs of the recipient

A survey by Gartner Consulting on E-mail users' perception of Spam found that 83% of the more than 13,100 respondents dislike Spam (Gartner Consulting 1999). E-mail users dislike Spam because of additional cost they have to incur in dealing with them. They have to download the Spam, to read through it to determine whether the content is useful and to delete it if it is not useful. The aggregate loss of time and money in aggregate taken in dealing with these messages might be huge. With the growing dependence of users on the Internet and e-mail for communications, the phenomenon of Spam can seriously hamper the development of the digital economy and society by undermining user confidence in online activities.

Equip Technology & CipherTrust (2004, p.1) found that the average E-mail user receives up to 70 E-mails a day. According to Ferris Group, the average employee spends 30 minutes each day dealing with Spam. (Equip Technology & CipherTrust 2004, p.2). A December 2004 survey suggested that internet users spend an average of 10 working days per year dealing with spam, and at least some industry analysts estimate that the 2005 cost of spam to business due to lost productivity and additional network maintenance costs will be around \$50 billion for the year (Zeller 2005, p.3).

Associated with Spam, the primary technical costs are the bandwidth and storage that it uses. A report by the European Union estimates the global bandwidth costs of Spam at \$8-10 billion annually (Equip Technology & CipherTrust 2004, p.2).

The influx of Spam has caused many people and organizations to deploy some form of anti-Spam solution. A European Commission study estimates that the costs associated with these solutions might come up to 10 billion Euro per year worldwide (Gauthronet & Drouard 2001). Another study finds that the longer an E-mail user retains an E-mail account, the more likely he will be spammed (Gartner Consulting 1999, p. 4).

E-mail users also face a second order cost of overloading at the mailbox. Spam degrades E-mail services, fills up users' mailbox with useless information, and decreases the usefulness of the E-mail service.

The impact of Spam on E-mail service providers is tremendous, as each ESP serves many E-mail users. The more Spam there is, the higher will the bandwidth be required. Similarly, a faster and larger capacity server is needed to process the incoming E-mails and Spam. It is not impossible that an ESP's network is forced to the point of a shut down because of Spam (Goodman 2000).

In order to cope with increasing amount of Spam, ESPs have resorted to filtering and blocking Spam on the users' behalf. Even web-based E-mail services, which derives revenue from banner advertisements that appear when a user reads his E-mails, provide Spam filtering services in order to retain users. GartnerConsulting's survey finds that most E-mail users look favorably at an ESP that offers a Spam filtering service as part of its program (Gartner Consulting 1999, p. 10).

However, a survey in 1998 finds that the ISPs' additional cost of hiring Spam-fighters range from a few hundred thousand US dollars to more than a million per year (Dern 1998).

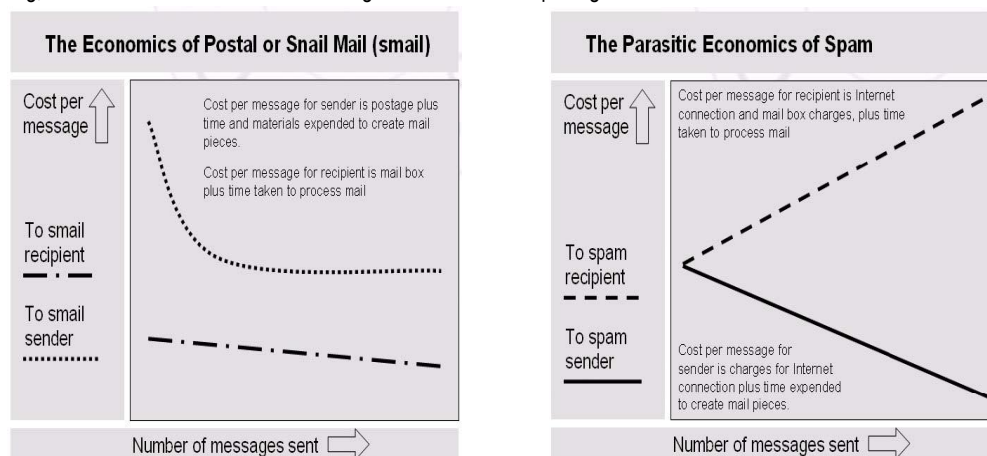
In addition, the third parties bear part of the social cost of Spam. As Spammers usually use a fake E-mail address, and some of the recipient addresses are not valid, bounced messages are relayed back and forth a couple of times between the sender's ESP and the recipient's root server. Bounced Spam further takes up unnecessary network bandwidth. False sender's or reply address poses further problem to third parties. If the reply address belongs to a third party, he will also be unwittingly flamed by angered Spammed recipients.

3 Comparison between traditional mail and E-mail

To better understand the problem of the costs of the senders and the recipients, Cobb (2003) compared the situation between traditional

mail and Spam. He suggested the concept of “the parasitic economics of Spam,” meaning that the act of sending a message costs the sender less than it costs all other parties impacted by the sending of the message (Cobb 2003, p.2).

Cobb compared the E-mail with the traditional mail that the postal service delivers and concluded that the cost per message for traditional mail declines as you increase volume, due to printing and handling efficiencies, bulk postage rates, and so on. But after a certain point it stops declining, because there are limits to the sliding scale for bulk mail postage. This can be shown as a curve that flattens out.



Source: Cobb (2003), p.2

Source: Cobb (2003), p. 3

The per message cost of traditional mail to the recipient is low to begin with, and relatively fixed. By contrast, most E-mail users check it multiple times per day, and Spammers are constantly coming up with new ways to make their messages look like legitimate E-mail. This means that sorting is a nontrivial task performed multiple times per day.

On the contrary, per message costs for Spammers start out low and decrease rapidly with volume. In reality, some Spammers pay nothing for sending their messages, hijacking resources that belong to others.

VI Non-legislative solutions to Spam

The popular approaches to managing Spam fall roughly into four categories, technological, market, educational, and regulatory. The first three approaches are analyzed in this section, and the regulatory approach is analyzed in the next section.

1 Technological solutions

Technological solutions to Spam can be divided into two types, i.e. the inbound solution and the outbound solution. Most previous work on Spam has focused on stopping inbound Spam (Dwork & Naor 1993; Naor 1996; Sahami et al 1998; Johanson 2002). Popular approaches include computational approach (Dwork 1993, Johanson 2002), challenge response (including HIPs, Naor 1996; CAPTCHA, Blum et al 2000), rule-based filters (Cranor & LaMacchia 1998), Bayesian filters, and community classification. The best known outbound solution is the adoption of HIP idea (Hansell 2003a).

Unfortunately, no existing solution has been completely effective and most devolve to a technological arms race. Using a single approach tends to result in administrators either “setting the bar too low” and letting in too many unwanted messages, or “setting the bar too high” and blocking legitimate E-mail (Cooley 2004). As long as marginal costs of sending remain low, a Spammer can simply send variation after variation to thwart a filter, eating up bandwidth along the way. When Spam is a negative externality to its recipients, E-mail users will choose to lower their loss of time by filtering mechanisms. Similarly, E-mail service providers may also lower the negative externality by refusing to relay Spam E-mails. Blocking and filtering systems take time and money to install and administer, and they are not without serious and potentially costly side effects of blocking messages in error (Khong 2004).

2 Market solutions

A few articles have explored marketbased mechanisms for allocating receiver attention (Kraut et al 2003; Fahlman 2002; Zandt 2003). Such mechanisms include stamps, surcharges on communication, and auctions. These are promising in that they shift the burden of screening from recipients to senders who know more about message content. One such proposal, focusing on sender surcharges, benefits most recipients and all senders by forcing them to collectively stop overexploiting receiver attention (Zandt 2003). Senders always benefit if either surcharges are rebated to the community, or more accurate recipient profiling allows senders to target more selectively. Shortcomings of focusing on senders include voluntary participation in surcharge mechanisms and also the ability to lie about content ex ante in order to elevate interest.

An experimental investigation of pricing recipient attention via E-mail postage found that charging does cause senders to be more selective and to send fewer messages (Kraut et al 2004). In particular, variable rate usage charges reduced communication more than flat rate access charges.

One well-designed mechanism is outlined by Fahlman in (Fahlman 2002) and more casually in (Ayres & Nalebuff 2003). The main observation is that communications media, such as E-mail, telephone and instant messaging, allow one person to interrupt another and obtain

their attention. Fahlman proposes giving recipients the ability to sell 'interrupt rights' to senders. Strangers must make a binding offer for the privilege of diverting a recipient's attention; they agree to pay an 'interrupt fee'.

3 Education of end users

It is becoming increasingly important that companies recognise the importance of educating end users about Spam and how to recognise and deal with it. A Yahoo survey showing that over 56% of users are unwittingly replying to Spam, the cost in terms of lost hours of productivity is clear. Users must also be made to understand that "friendly fire" also constitutes Spam, and that they should refrain from using company E-mail for these purposes. Furthermore, if users reply to Spam, they often do not realise that this action will probably expose them to a hundred other databases or sources of Spam.

VII Regulatory solutions

1 Opt-in vs. opt-out

1.1 Different legislative models

In regard to how to define the consent of a data subject which is required to obtain to send such Spam e-mails, there are two methods, "opt-in" and "opt-out".

The European Union has adopted an "opt-in" approach for commercial communications by E-mail, by way of Directive 2002/58/EC, which is an integral part of the new, wider European Community (EC) regulatory framework on electronic communications.

The Directive contains three basic principles with regard to unsolicited commercial communications. Firstly, according to Art. 13(1) of the Privacy and Electronic Communications Directive member states are required to prohibit the sending of unsolicited commercial communications by fax, E-mail, or other electronic messaging systems such as SMS and Multi-media Messaging Service (MMS) unless the prior consent of the person has been obtained. This regime is applicable for marketing to individuals but member states can extend the scope to marketing communications to businesses. There is a limited exception from the opt-in system for existing customers (Art. 13 (2)) for the use of contact details obtained from customers in the context of a sale, but it may only be used by the same legal person for the marketing of 'similar' products or services and provide an explicit opt-out is offered at the time of collection and with each subsequent message. Secondly, the disguise of identity of the sender is prohibited. Thirdly, direct marketing messages must include a valid return address where persons may opt-out.

The implementation of this Directive establishes a similar legislative model in all the European Union member states. The Directive states that users must opt in to receive unsolicited electronic communications for marketing purposes (Sipior, Ward & Bonner 2004, 62). Countries where "Opt-in" legislation has been enacted include Austria, Denmark, Finland, Germany, Greece, Hungary, Italy, Norway, Poland, Slovenia, and Spain. Countries where "Opt-in" legislation is under consideration include Belgium, France, and Sweden. Finland, France and the UK do not require opt-in when the recipient is a registered legal person (Sipior Ward & Bonner 2004, 62).

This Directive should be interpreted together with the 'general' Directive 95/46/EC, where concepts like consent, etc. are defined. In addition, other European Community law provisions may be applicable to unsolicited communications in relation to e.g. misleading advertising, harvesting, hacking.¹

In the Asia-Pacific region, Australia has been the first to introduce opt-in explicitly in their law. The NOIE Report recommending opt-in legislation was followed by the adoption of the Spam Bill 2003 by the Australian Parliament. Australia exempts government bodies, political parties, religious organisations, charities and educational institutions from respecting the opt-in requirement. There is no specific regulation on Spam in Canada to date, though an opt-in approach has been adopted by applying existing law. In Canada, under the Personal Information Protection and Electronic Documents Act electronic mail addresses are considered personal information. Thus, the collection and use without consent of personal information, such as E-mail address, could run counter to the requirements of the Act (Industry Canada 1999). Recent changes to the Federal Law of Consumer Protection in Mexico reflect the adoption of an opt-out approach. Mexican consumers are entitled to prevent specific businesses from disturbing them at home or at the workplace, or via E-mail, and from unauthorised transmission of personal data to third parties. To date, Korea and Japan have adopted an opt-out approach. However, the Ministry of Information and Communication (MIC) in Korea announced the introduction of opt-in for mobile phone services.

The 2004 US CAN-SPAM Act² took effect, which superseded more than 30 state laws covering Spam. The legislation adopts an opt-out approach. Section 5 of the Act requires the following that all commercial E-mail must contain a valid opt-out mechanism, opt-out requests must be honored within 10 business days, sender must include a valid physical postal address, E-mail must provide a clear notice that it is an advertisement, E-mail must provide an operative return address, senders must avoid false, deceptive, or misleading E-mail transmission information or subject lines, and that senders must label sexually-oriented messages.

1.2 Economic analysis of different models

Opt-out approach is based on the idea of limited right of Spammers to send Spam. The central economic argument for this approach is

1 For example, Directive 2000/31/EC, which includes provisions for transparency in relation to E-mail marketing, notably requiring that commercial communications must be identifiable as such.

2 "Controlling the Assault of Non-solicited Pornography and Marketing Act", CAN-SPAM Act of 2003 (Pub. L. 108-187, S. 877).

cost reduction of the opt-out process. It does not take into account the possibility of a social loss when Spamming is done inefficiently. Neither does it induce Spammers to send Spam in an efficient manner (Coalition Against Unsolicited Commercial E-mail 2001; Scruggs & Anderson 1999). From an economic point of view, opt-out is only efficient under very strict conditions. The opt-out approach is usually inefficient (Khong 2004).

Under the opt-in approach, Spammers do not have a right to send unsolicited Spam, and this right is protected by a property rule. Taken that statutory or punitive damages are high enough to compensate for rational apathy, Spammers are induced not to send unsolicited Spam (Khong 2004). If E-mail users as a group could negotiate in a Coasean way with the Spammer, an efficient outcome can be achieved. But because E-mail users are a large and dispersed group, organizing them is costly (Khong 2004). For the same reason, opt-in laws are not common because of the inability of E-mail users to organize as a pressure group. The result is the same if advertising yields increasingly returns to scale. Spam is still not social welfare maximizing, although welfare is increased compared to the previous case. This is so because the gains by subscribers are not internalized by the Spammer (Khong 2004). As Gahran (2000) summarized that, the main advantages of opt-in e-mail services are timeliness, convenience, and control.

2 Labelling

Labelling consists of displaying standard identifying labels in the subject line or header such as "ADV" (advertisement), "ADLT" (adult-only; if it concerns material intended for those 18 years of age and older). With regard to labelling, Finland, Japan, Korea, Norway, Poland, the UK, and the US require senders to label certain kinds of messages, but others like Australia, Denmark, France, Germany, and Italy do not require it.

Many states in the US require a label in the subject line of an E-mail that will alert recipients that the message is an advertisement. This includes three modes: unsolicited sexually explicit messages must contain a label of "ADV: ADULT", "ADV: ADLT", "ADULT ADVERTISEMENT", "ADV: ADULT ADVERTISEMENT" at the beginning of the subject line;¹ unsolicited commercial E-mail messages must contain a label of "ADV:" or "ADVERTISEMENT".² The laws prohibit false, deceptive, or misleading subject lines.³

3 Identity

Regulation may include the prohibition of false sender identities or addresses; false headers or misleading information in the subject line, or disregarding an opt-out request through technical manipulation; unauthorised access or falsification of routing information or misrepresentation of information related to the identification of the point of origin or the transmission path; and the use of a third party's Internet domain name without permission.

Concerning the real identity of senders, the provision of opt-out in messages, and false information in headers and messages, quite a few countries have similar approaches. Australia, Belgium, Italy, Mexico, Netherlands, and Poland, indicated requiring the real identity and real address of a sender in their messages. The situation is similar regarding the opt-out requirement in messages. Denmark, Finland, Germany, Italy, Korea, and the UK have a regulation in which opt-out is required in messages so that recipients are able to oppose receiving further messages from the sender. France, Mexico, Norway and Poland do not require this. A number of countries prohibit false information in headers and messages, including Australia, Denmark, France, Italy, Poland and the US.

In the US, some states have taken steps to criminalize the act of sending unsolicited bulk E-mail containing false, falsified or missing routing information, or misrepresent or obscure the point of origin or routing information.⁴ Some states prohibit the sale, distribution, and possession with intent to sell software that is designed to falsify routing information.⁵ Some states outlaw unsolicited commercial E-mail using a third party's Internet address or domain name without permission.⁶ Some states require that the unsolicited commercial E-mail must include the sender's name, street address, and E-mail address, along with opt-out instructions.⁷

4 Address harvesting and do-not-Spam list

Harvesting E-mail addresses from websites can be prohibited and software products used for collecting E-mail addresses, transmitting bulk E-mail and falsifying return addresses (Spamware) can be banned or controlled. Regarding the use of Spamware, Australia, France, Italy, Japan,

1 As in Alaska, Arkansas, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Missouri, New Mexico, North Dakota, Oklahoma, Pennsylvania, South Dakota, Tennessee, Texas, Utah, and Wisconsin.

2 As in Arizona, Colorado, Michigan, and Nevada.

3 As in Arizona, Illinois, Indiana, Kansas, Maryland, Minnesota, Missouri, North Dakota, Oklahoma, Pennsylvania, South Dakota, Texas, Washington, West Virginia, and Wyoming.

4 As in Arizona, Arkansas, Colorado, Connecticut, Delaware, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming.

5 As in Arkansas, Connecticut, Delaware, Illinois, Kansas, Louisiana, Michigan, Nevada, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Virginia, and West Virginia.

6 As in Arizona, Arkansas, Colorado, Idaho, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Minnesota, North Dakota, Oklahoma, Pennsylvania, Rhode Island, Texas, Washington, West Virginia, and Wyoming.

7 Arkansas, Colorado, Indiana, Iowa, Kansas, Maine, Minnesota, Missouri, Nevada, new Mexico, Ohio, Oklahoma, Rhode Island, Tennessee, and Utah.

Korea, and Spain have a regulation which prohibits the use of Spamware for the purpose of Spamming, while others such as Denmark, Finland, Germany, and the UK do not. The US prohibits the harvesting of E-mail addresses, dictionary attacks and spoofing.

With regard to do-not-Spam lists, most countries do not require the operation of do-not Spam lists, with the exception of Austria and Korea. However, the UK, even though it is not a statutory requirement, opt-out registers have been operated under industry codes of practice.

5 Criminal sanctions and civil remedies

5.1 Criminal sanctions

Sanctions for violation of Spam laws and regulations are getting tougher. Some countries such as Korea have considerably increased existing fines imposed on Spammers by amending existing regulations. Others like Italy impose not only fines on Spammers but also prison terms (OECD 2004).

In some of the US states, Spam has been criminalized by state laws, such as Colorado, Nevada, Pennsylvania, Connecticut, Delaware, Louisiana, North Carolina, and Virginia. In some other jurisdictions without statutes regulating commercial Spam, unsolicited E-mail is usually regulated with reference to harassment, stalking, and sexually explicit communication to minors, such as in Hawaii, Wisconsin, and Maryland. The Section 4 of 2004 CAN-SPAM Act prohibits hiding E-mail origin using other computers (hacking and relaying), false or misleading E-mail header information, deception in registration of E-mail and domain names, and ownership of IP addresses. Under the Act, violations of the provisions above can result in fines and imprisonment of between 1 and 5 years depending on the seriousness of the violation and other factors. Section 4 of the Act provides for forfeiture of property used in connection with the commission of the offense, or gained in or traceable to the commission of the offense.

In exploring the sanctions for Spam, there are two problems deserving reconsidered.

First, it is generally argued that the fine is better than imprisonment for several reasons, assuming the deterrence costs are the same (See generally Garoupa 2003). If the hacker works, he will learn some new skills and perhaps be able to become more attached to the legitimate labor market (See generally Garoupa 2003). However, given that they are long specified in computer science, and deprived the chances of further study, their knowledge and skills will become outdated after several months or years. If the fine is used to compensate the Spam victims, then their loss will be reduced, and the cost to society of his or her crime will be reduced. This is more efficient than having him or her in jail, which doesn't help the victims (See generally Garoupa 2003). However, in the case of Spam, there are always too many victims (thousands or millions), it is impossible to pay each victim. Thus, the loss of the victim become a pure social loss, and cannot be recovered from the criminal.

Second, prosecutors face a number of costs when bringing legal action against Spammers. The cost of tracking down Spammers, the costs of actually litigating a trial once a target has been identified, and any negative externalities borne by society as a result of prosecution, the cost to those legitimate businesses must be taken into account (Prince 2004). The expected effectiveness of an anti-Spam law is determined by a number of quantifiable factors, such as the potential benefit to society from a single successful prosecution, the costs of identifying a Spammer to be prosecuted and the costs of actually bringing the prosecution against him or her, the likelihood of success at trial, and any external costs to society that arise as a byproduct of prosecution (Prince 2004). In order to justify prosecuting a Spammer, the expected effectiveness quotient must be as high as possible (Prince 2004). For an anti-Spam law to be a successful deterrent to Spammers, it must be drafted to increase the benefit from a successful prosecution, decrease the cost of identifying a Spammer, decrease the cost of prosecution, increase the probability of success at trial, or decrease any external costs to society from investigating and bringing a trial (Prince 2004).

Although there are cases of harsh criminal sanctions such as that a Virginian spammer was sentenced to 9 years in prison for sending 10 million E-mails each day, and cases of large damages, such as that another spammer was sued by AOL for 7 million dollar, Spamhaus estimates that by the summer of 2006 spam will account for 95% of all e-mails sent and the problem will not be alleviated (Wakefiled 2005).

5.2 Civil remedies

It is also possible to take civil actions against spam senders. First of all, because the ISPs' systems are repeatedly burdened by huge volume mailings, they can incur noteworthy cost. Thus, they have the choice of seeking financial compensation through civil action. Generally, civil laws that apply to damages resulting from wrongful actions or breaches of contract would apply to conventional and online activities equally. The scope of contract liability is largely a matter for ISPs and other intermediaries, who are free to set the terms of contracts with their subscribers. Many existing contracts incorporate anti-spamming conditions (Ferguson & Piragoff, 1997).

Another form of civil actions can also protect recipients from Spamming. Damages are a good deterrent against spam. Laws of some the US states provide statutory damages to individuals and ESPs. These damages vary from US\$10 per message in Colorado and Iowa to US\$500 in Rhode Island. Some states also allow recovery of actual damages to spam recipients and network administrators. Section 5 of the US CAN-SPAM Act. Although the Act does not provide a civil cause of action for individuals against Spammers, it empowers attorneys general of each state to pursue violators of certain parts of Section 5 on behalf of the residents of its state. A state attorney general can pursue money damages, injunctive relief to stop further violations of the Act, or statutory damages which can total to \$2,000,000 or more for inclusion of false or misleading transmission information, or if circumstances support a finding of aggravated damages. Statutory damages can reach up to \$250 per address to which an E-mail is sent. A court may treble damages if it finds aggravating circumstances, and may in its discretion award attorney

fees for successful actions. Others who have a civil cause of action under the Act include ISP's and certain federal agencies. ISP's are provided a civil cause of action against violators of certain sections of the Act. Finally, the Act generally can be enforced by a variety of federal agencies noted in the Act when the actions or actors fall within the agency's purview.

6 International co-operation

As a global problem, the practical problems in finding wrongdoers, establishing jurisdiction, and enforcing remedies, investigation and prosecution of cases involving Spam are extremely difficult. The different approaches among countries may cause further difficulties to implement effective solutions worldwide. The Spam outside their territories will be outside their reach.

There have been a number of international initiatives to address the problem of cross-border scams. In particular, in June 2003, the OECD adopted new guidelines to foster international co-operation against cross-border fraud and deception (OECD 2003). Spam messages that contain deceptive or fraudulent representations may fall within the scope of the guidelines, offering the prospect of putting into play the framework for enforcement co-operation outlined by the guidelines.

Recent trends in international co-operation have been between industries, organisations and the consumer or citizen, and between industries and government. Important multi-lateral organisations include the OECD, ITU, APEC, ICANN and ICPEN. International co-operation which is multi-pronged needs to include various different communities in order to be effective (OECD 2004). In dealing with the problem of Spam, the new-styled international co-operation is an urgent call. As of 2005, International Council on Internet Communications was formed to coordinate international efforts to stop spammers (NewsTarget 2005). Given Spam is still in its rapid developing stage, we cannot expect any of such institutions are able to solve the problem in a predictable period.

7 Regulatory solution revisited

The fact that the amount of Spam is rising despite the number of world legislations restraining it suggests that legislation is not a sure solution to the Spam problem. Certain regulations, such as a labeling "ADV" in message headers, have not proven effective (FTC 2003b). Some organizations such as the Direct Marketing Association (DMA) argue that only legitimate law-abiding marketers would actually use ADV labeling, which voluntarily subjects them to mass filtering. Others also question the effectiveness of government-operated nationwide "do-not-E-mail registries", because such lists would only punish those reputable marketers who comply with them. On the other hand, opt-out is not used by most consumers, who fear that opt-out will confirm their address to Spammers; uncertainty as to whether opt-out will work; doubt that opt-out will be honored (ePrivacy Group 2003).

There are a number of limitations to the effectiveness of law enforcement against Spamming. These include low cost-effectiveness, difficulty in tracking Spammers, difficulty in collecting evidence across borders, varying regulations between states or countries, etc. Some interpretations of existing privacy legislation can also raise obstacles to effective law enforcement, if they do not allow law enforcement to have access to information about alleged Spammers.

Since the first anti-Spam law worldwide was passed in 1997, at least 75 governments around the world have passed anti-Spam laws (Sorkin 2004; Direct Marketing Association 2004). The empirical evidence for the failure is quite clear. In 1997, the average e-mail user received approximately one unsolicited commercial e-mail message per week (Cranor & LaMacchia 1998). By 2003, the average e-mail user received 25 such messages daily (InsightExpress/UnSpam 2003) While that is an astounding 175-fold increase in merely six years, the averages vastly understate the problem for many active e-mail users, some of whom receive literally thousands of Spam messages each day (InsightExpress/UnSpam 2003) Spammers routinely flout the law because the risk of prosecution is so low. Three months after the passage of the US CAN-SPAM Act,¹ only three per cent of Spam messages complied with its requirements (McGuire 2004). What is worse is that today the compliance rate is down to a scant one per cent (McGuire 2004). More pessimistic perspective shows that "*Law Barring Junk E-Mail Allows a Flood Instead*" (Zeller 2005). According to Jared Blank, "The laws are nice in theory, but actually going after and tracking down spammers is extraordinarily difficult." (Levine 2003).

VIII Conclusions

Spammers are motivated by benefits from spamming that are greater than other kind of direct mailing. Any previous single solution cannot work alone to solve the problem. Comprehensive mechanisms must be established to protect the recipients with more effective anti-Spam systems, and to impose criminal and civil liability on the sender.

References

1. Ayres, I., & Nalebuff, B. (2003). Want to Call Me? Pay Me! In Wall Street Journal, 8 Oct. 2003.
2. Batista, Elisa. (2000). A Fight to Ban Cellphone Spam, Wired News, 6 July 2000.
3. Becker, G. (1968). "Crime and Punishment: An Economic Approach," Journal of Political Economy 76, 169-217.
4. Blum, M., von Ahn, L. A., Langford, J., & Hopper, N. (2000). The CAPTCHA Project: Completely Automatic Public Turing Test to Tell Computers and Humans Apart, Nov. 2000, at <http://www.captcha.net> (accessed 28 April 2005).
5. Boldt, Martin, Carlsson, Bengt, & Jacobsson, Andreas. (2004). Exploring Spyware Effects, at http://psi.bth.se/mbo/exploring_spyware_effects-

¹ See 15 USC. § 7705. CAN-SPAM stands for the "Controlling the Assault of Non-Solicited Pornography and Aggressive Marketing." It was signed into law 16 Dec. 2003 and became effective 1 Jan. 2004.

- nordsec2004.pdf (accessed 28 April 2005).
6. Coalition against Unsolicited Commercial E-mail. (2001). CAUCE Does the Math—Why Can't the Marketing Industry? 15 May 2001, at <http://www.cauce.org/pressreleases/math.shtml> (accessed 28 April 2005).
 7. Cobb, Steven. (2003). The Economics of Spam, at http://www.spamhelp.org/articles/economics_of_spam.pdf (accessed 28 April 2005).
 8. Cooley, A. L. (2004). The Cocktail Approach to Spam Protection, Network Security White paper.
 9. Cranor, L. F. & LaMacchia, B. A. (1998). Spam! Communications of the ACM. 41(8), pp. 74-83.
 10. Dem, Daniel P. (1998). Postage Due on Junk E-mail: Spam Costs Internet Millions Every Month, Internet Week, 4 May 1998.
 11. Direct Marketing Association, Executive Summary of International Spam Laws, at <http://www.the-dma.org/antispam/spamlaws.html> (accessed 28 April 2005).
 12. Dwork, C., & Naor, M. (1993). Pricing via Processing or Combating Junk Mail. In Lecture Notes in Computer Science 740 (Proceedings of CRYPTO'92), pp. 137–147, 1993.
 13. Dwork, C., Goldberg, A., & Naor, M. (2003). On Memory-bound Functions for Fighting Spam, Proceedings of the 23rd Annual International Cryptology Conference (CRYPTO 2003), pp. 426-444, Santa Barbara, CA, Aug. 2003.
 14. EquiP Technology and CipherTrust. (2004). Spam and Productivity Theft- a Growing Concern for UK PLC. A Report by EquiP Technology and CipherTrust, at <http://www.apig.org.uk/equipandciphertrustevidence.doc> (accessed 28 April 2005).
 15. Fahlman, S. E. (2002). Selling Interrupt Rights: A Way to Control Unwanted E-mail and Telephone Calls. IBM Systems Journal, 41(4):759–766, 2002.
 16. Federal Trade Commission, National Do-Not-E-mail Report to Congress, 15 June 2004.
 17. Federal Trade Commission. (1998). FTC Names Its Dirty Dozens: 12 Scams Most Likely to Arrive via Bulk E-mail, FTC Consumer Alert, July 1998.
 18. Ferguson, Peter, & Piragoff, Donald K. (1997). Internet and Bulk Unsolicited Electronic Mail, at [http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/SPAM_1997En.pdf/\\$FILE/SPAM_1997En.pdf](http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/SPAM_1997En.pdf/$FILE/SPAM_1997En.pdf) (accessed 28 April 2005).
 19. Foster, Ed. (2000). Viral Marketing Goes One Step too Far—To a Place Where Friends Spam Friends, InfoWorld, 7 Feb. 2000.
 20. Gahrn, Amy. (2000). Investor relations Content that Works, 10 March 2000, at <http://www.contentious.com/articles/V2/2-7/feature2-7.html> (accessed 28 April 2005).
 21. Garoupa, Nuno. (2004). An Economic Analysis of Criminal Law, at http://esnie.u-paris10.fr/pdf/textes_2004/Garoupa_criminalaw01.pdf (accessed 28 April 2005).
 22. Gartner Consulting. (1999). ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition, Gartner Consulting, 14 June 1999.
 23. Gauthronet, Serge, & Drouard, Etienne. (2001). Unsolicited Commercial Communications and Data Protection (Brussels: Commission of the European Communities, Internal Market Directorate General, 2001), Contract no. ETD/99/B5-3000/E/96.
 24. Goodman, Peter S. (2000). Verizon Online User's E-mail Problems Persist, Washington Post, 13 Dec. 2000, p. E01.
 25. Griffin, P. (2003). Spammers Remain Unrepentant as They Make Money, in the New Zealand Herald, 21 March 2003.
 26. Grimes, Anne. (2003). Digits: Spam pays, The Wall Street Journal, 22 May 2003, p. B3.
 27. Hansell, Saul. (2003a). Internet is Losing Ground in Battle against Spam. The New York Times. 22 April 2003, p. 1.
 28. Hansell, Saul. (2003b). The High, Really High or Incredibly High Cost of Spam, The New York Times, 29 July, 2003.
 29. Hise, Phaedra. (1999). Mom Spam: The Cyber-Scourge of Families Everywhere, Salon, 20 Dec. 1999, at <http://www.salon.com/mwt/feature/1999/12/20/Spam/> (accessed 28 April 2005).
 30. IMT Strategies (2001). Raising the Stakes in Permission Marketing, Stamford, CT USA, at <http://www.imtstrategies.com/download/TI13.01.pdf/> (accessed 28 April 2005).
 31. Industry Canada. (1999). Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy, July 1999, at <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html> (accessed 28 April 2005).
 32. Infoworld. (2003). What is the Worst IT Disaster of the Last Year, July 2003.
 33. InsightExpress/UnSpam. (2003). Comprehensive Spam Survey, 12 Oct. 2003, at http://www.unSpam.com/fight_Spam/information/survey_personal.html (accessed 28 April 2005).
 34. ITU (International Telecommunication Union). (2004a). Meeting Announcement: ITU WSIS Thematic Meeting on Countering Spam, CICC, Geneva, 7–9 July 2004.
 35. ITU (International Telecommunication Union). (2004b). Council Working Group on the World Summit on the Information Society, Document WG-WSIS 7/13-E, 2004.
 36. Johansson, E. S. (2002). Camram, 2002, at <http://www.camram.org> (accessed 28 April 2005).
 37. Kelly, J.S. (2002). A Brief History of Spam, at <http://www-106.ibm.com/developerworks/linux/library/l-spam/l-spam.html> (accessed 28 April 2005).
 38. Khong, D.W.K. (2004). An Economic Analysis of Spam Law, Erasmus Law and Economics Review, 1 (Feb. 2004): pp. 23–45.
 39. Kraut, R., Sunder, S., Morris, J., Cronin, M., & Filer, D. (2003). Markets for attention: Will postage for E-mail help? In ACM Conference on CSCW, pp. 206–215, 2003.
 40. Kraut, R.E., Sunder, S., Telang, R., & Morris, J. (2004). Pricing Electronic Mail to Solve the Problem of Spam, at <http://www.econ.upf.es/docs/seminars/sunder.pdf> (accessed 28 April 2005).
 41. Levine, Jessica. (2003). Spam and the Law, PC Magazine, 25 Feb. 2003.
 42. MAPS (Mail Abuse Prevention System). (2004). Definition of Spam, at <http://www.mail-abuse.comSpam-def.html> (accessed 28 April 2005).
 43. Marlin, A.S. (2000). First Amendment Is Obstacle to Spam Legislation, CNN.com, at <http://archives.cnn.com/2000/TECH/computing/06/09/amend.spam.idg/index.html> (accessed 28 April 2005).
 44. McGuire, David. (2004). Report: More Spam Violates Law, Washington Post, 9 June 2004.
 45. Moran, J. M. (2002). Spam King Living High in the Bayou, in The Hartford Courant, 30 June 2002.
 46. Naor, M. (1996). Verification of a Human in the Loop or Identification via the Turing Test, at <http://www.wisdom.weizmann.ac.il/~naor/PAPERS/>

- (accessed 28 April 2005).
47. NewsTarget. (2005). New international anti-spam council pledges to fight spam around the world, 28 April 2005, at http://www.wired.com/news/technology/0,1282,64383,00.html?tw=wn_tophead_5 (accessed 28 April 2005).
 48. Niall, Jim (2000). The E-mail Marketing Dialogue, Forrester Report, Cambridge.
 49. OECD. (2003). OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, June 2003.
 50. OECD. (2004). 2nd OECD Workshop on Spam: Report of the Workshop. JT00174847.
 51. Peppers, D. & Rogers, M. (2000). E-mail Marketing Maximized, Peppers, Stamford, C.A.
 52. Pool, I., Inose, H., Takasaki, N. & Hurwitz, R. (1984). Communication flows: A Census in the United States and Japan. New York: North-Holland.
 53. Prince, M. (2004). How to Craft an Effective Anti-Spam Law, June 2004, at <http://www.itu.int/spamH> (accessed 28 April 2005).
 54. Radical group, The Radical Group, Inc. Release Q1 2005 Market Numbers Update, 25 April 2005.
 55. Sahami, M., Dumais, S., Heckerman, D., & Horvitz, E. (1998). A Bayesian Approach to Filtering Junk E-mail. In AAAI '98 Workshop on Learning for Text Categorization, July 1998.
 56. Scruggs, D., & Anderson, H. (1999) Sometimes the Messenger Should Be Shot: Building a Spam-free E-mail Marketing Program, 1999, at <http://www.messagemedia.com/> (accessed 28 April 2005).
 57. Simon, H. A. (1982). Designing Organizations for an Information-rich World: Models of Bounded Rationality, MIT Press. pp. 171-185.
 58. Sipior, J. C., Ward, B. T., and Bonner, P. G.. (2004). Should Spam Be on the Menu? Communications of the ACM, vol. 47, no. 6, 59-63 (June 2004).
 59. Sorkin, David E. (2004). Spam Laws, at <http://www.spamlaws.com/> (accessed 28 April 2005).
 60. Templeton. (2003). Origin of the Term "Spam" to Mean Net Abuse, at <http://www.templetons.com/brad/spamterm.html> (accessed 28 April 2005).
 61. Wakefield, Jane, UK laws are failing to deter spam, BBC News, 21 April 2005, at <http://news.bbc.co.uk/1/hi/technology/4466053.stm> (accessed 28 April 2005).
 62. Wendland, M. (2002). Spam King Lives Large off Others' E-mail Troubles, in The Detroit Free Press, 22 Nov. 2002.
 63. Wreden, N. (1999), Mapping the Frontiers on E-mail Marketing, Harvard Management Communication Letter, 9 Jan. 1999.
 64. Wright, N. D., & Bolting, C. P. (2001), Marketing via E-mail: Maximizing its Effectiveness Without Resorting to Spam, working paper, James Madison University.
 65. WSIS (World Summit of Information Society). (2003). Declaration of Principles-Building the Information Society: a Global Challenge in the New Millennium, World Summit of Information Society, 2003.
 66. Zandt, T. V. (2003). Information Overload in a Network of Targeted Communication, RAND.
 67. Zeller, T., Jr. (2005). Law Barring Junk E-Mail Allows a Flood Instead, New York Times, nytimes.com, Feb. 2005.
 68. Wikipedia, Externalities, at <http://en.wikipedia.org/wiki/Externality> (accessed 28 April 2005).
 69. Amaditz, K. C. (1999). Canning "Spam" in Virginia: Model Legislation to Control Junk E-mail, Virginia Journal of Law and Technology, Vol. 4, Issue 4, 1999.